REMARKS

Applicant submits this Response to the Office Action mailed August 9, 2005. Applicant has amended claims 1, 6, 23, 24, 29 and 36. Claims 1-36 are currently pending. No new matter has been added.

In the Office Action, the Examiner has rejected claims 6 and 23 under 35 U.S.C. § 112, ¶ 2, as lacking antecedent basis. Applicant has amended claims 6 and 23 to correct the errors identified by the Examiner as the basis for these rejections. Applicant thus respectfully requests that the Examiner withdraw these rejections.

The Examiner has also rejected claims 1-36 under 35 U.S. § 103(a) as being unpatentable over U.S. Patent No. 5,590,199 to Krajewski, Jr. et al. ("Krajewski") in view of U.S. Patent No. 5,005,200 to Fischer ("Fischer"). Applicant traverses these rejections and requests reconsideration of these claims, based on the following.[1]

Krajewski describes a system that includes a user workstation, an authorization server and a number of service providers, all connected over a network. (Krajewski, col. 5, lines 46-53.) The user is able to couple a coprocessor device (described as a "smart card") to the user workstation; the smart card is programmed with an encrypted user key. (Id., col. 3, lines 54-62.) In operation, the system described in Krajewski works in three phases:

> (1) The user enters a user ID at the user workstation, which is sent to the Kerberos authentication server to obtain a Kerberos ticket granting service (TGS) ticket and an encrypted session key. The user then enters a password; if the password is correct, the session key is decrypted and stored in the smart card. (Id., col. 5, line 64 to col. 6, line 9.)
>
> (2) The user initiates a request for a service by sending the TGS ticket and an authenticator encrypted by the smart card to the Kerberos authentication server. The

[1] As Applicant's remarks with respect to the Examiner's rejections are sufficient to overcome these rejections, Applicant's silence as to assertions by the Examiner in the Office Action or certain requirements that may be applicable to such rejections (e.g., whether a reference constitutes prior art, motivation to combine references) is not a concession by Applicant that such assertions are accurate or such requirements have been met, and Applicant reserves the right to analyze and dispute such in the future.

authentication server returns a server ticket and an server session key to the user workstation, encrypted using the session key. The server session key is decrypted by the smart card. (Id. col. 6, lines 10-23.)

(3) The user workstation and smart card encrypt an authenticator for the server ticket, and the user workstation sends the server ticket and authenticator to the service. (Id., col. 6, lines 23-28.)

Krajewski summarizes that "all encryption and decryption required for access to the authorization server 32 or a network service 20 is done within the smart card." (Id., col. 6, lines 31-33.)

Fischer is cited by the Examiner as disclosing " a trusted authority creating and issuing a digital certificate to a claimant (network server), which reveals the public key of the user, which will be used to establish a secure connection (SSL)." Office Action, p. 4.)

In contrast, claim 1 recites a method of enhancing the security of a message sent by a principal from a client computer through a network server to a destination server that includes:

(a) obtaining by the client computer credentials for authorizing the principal from a validation center;
(b) establishing a first secure connection for exchanging data between the client and the network server;
(c) transmitting from the client computer to the network server over the first secure connection the principal-authenticating credentials and the message;
(d) transmitting the principal-authenticating credentials from the network server to the validation center;
(e) transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials;
(f) verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server;
(g) establishing a second secure connection for exchanging data between the network server and the destination server based on the digital certificate; and
(h) transmitting the message from the network server to the destination server over the second secure connection.

Krajewski and Fischer, either taken alone or in combination, do not teach or suggest such a method. For example, neither Krajewski nor Fischer describe "transmitting from the client computer to the network server over the first secure connection the principal-authenticating

credentials and the message," "transmitting the principal-authenticating credentials from the network server to the validation center," transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials," verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server," "establishing a second secure connection for exchanging data between the network server and the destination server based on the digital certificate," and "transmitting the message from the network server to the destination server over the second secure connection," as recited in claim 1. Notably, both Krajewski and Fischer lack any description of a "network server" that acts between a client computer, validation center and destination server, as recited in claim 1.

Applicant notes that in applying Krajewski to the elements of claim 1, the Examiner appears to map the claimed "client computer" to the "user workstation" in Krajewski, the claimed "network server" and "destination server" to the "system services" of Krajewski, and the claimed "validation center" to the "Kerberos authentication server" of Krajewski. Even if such mappings could be considered proper (which Applicant does not), Krajewski does not describe the performance of the steps of claim 1 between such entities. For example, Krajewski does not describe "transmitting the principal-authenticating credentials from the network server to the validation center"; the cited portion of Krajewski only describes transmission of a TGS ticket and session key from the user workstation to the KAS. Likewise, Krajewski does not describe "transmitting the message from the network server to the destination server over the second secure connection"; under the Examiner's interpretation, this element would be not exist in Krajewski, since the network server and the destination server are the same entity.

Applicant has made several clarifying amendments to claim 1 to emphasize the interactions between various elements. If the Examiner continues to believe that Krajewski and/or Fisher render the claims unpatentable, in the interests of advancing prosecution of this application, Applicant requests that the Examiner set forth in tabular form which structures in Krajewski and/or Fisher are analogous to the claimed elements and the transmissions/transactions by/between each structure that are applicable.

Based on the foregoing, Applicant believes claim 1 to be patentable over Krajewski and/or Fischer, and respectfully requests that the Examiner withdraw the rejection of claim 1. As claims 2-22 depend from claim 1, and therefore include all of the limitations of claim 1, Applicant believes claims 2-22 to be patentable over Krajewski and/or Fischer for at least the same reasons as claim 1,[2] and therefore respectfully requests that the Examiner withdraw the rejections of claims 2-22 as well.

Claim 36 recites a computer program product that includes a computer program for carrying out the process of claim 1. As noted above, Applicant believes claim 1 to be patentable over Krajewski and/or Fischer. Applicant therefore respectfully requests that the Examiner withdraw the rejection of claim 36 as well.

In further contrast to Krajewski and Fischer, claim 23 recites a method of providing a remote interactive login connection for a principal from a client computer through a network server to a destination server that includes:

(a) obtaining credentials for authorizing the principal from a validation center;
(b) establishing a first secure connection for exchanging data between the client and the network server;
(c) transmitting from the client computer to the network server over the first secure connection the principal-authenticating credentials;
(d) transmitting the principal-authenticating credentials from the network server to the validation center;
(e) transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials;
(f) verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server;
(g) establishing a second secure connection for exchanging data between the network server and the destination server based on the digital certificate; and
(h) executing a command interpreter in the destination server
wherein the command interpreter may execute commands sent by the client computer via the network server over the second secure connection.

Krajewski and Fischer, either taken alone or in combination, do not teach or suggest such a method. As noted above with respect to claim 1, neither Krajewski nor Fischer describe

[2] As Applicant's remarks with respect to the base independent claims are sufficient to overcome the Examiner's rejections of all claims dependent therefrom, Applicant's silence as to the Examiner's assertions with respect to dependent claims is not a concession by Applicant to the Examiner's assertions as to these claims, and Applicant reserves the right to analyze and dispute such assertions in the future.

"transmitting from the client computer to the network server over the first secure connection the principal-authenticating credentials and the message," "transmitting the principal-authenticating credentials from the network server to the validation center," transmitting permission data for the network server from the validation center to the network server based on the principal-authenticating credentials," verifying the authorization of the principal in the network server to access a digital certificate and issuing a digital certificate to the network server," "establishing a second secure connection for exchanging data between the network server and the destination server based on the digital certificate," and "executing a command interpreter in the destination server, wherein the command interpreter may execute commends sent by the client computer via the network server over the second secure connection," as recited in claim 23. Krajewski and Fischer lack any description of "network server" as recited in claim 23, which precludes any method steps involving such a network server. Accordingly, Applicant respectfully requests that the Examiner withdraw the rejection of claim 23.

In further contrast to Krajewski and Fischer, claim 24 recites a computer system for enhancing the security of one or more messages sent by a principal that includes:

> a client computer for transmitting principal-authenticating credentials and the one or more messages;
> a gateway computer operatively connected to the client computer, the gateway computer receiving principal-authenticating credentials and the one or more messages from the client computer;
> a validation computer operatively connected to the gateway computer and capable of receiving the principal-authenticating credentials from the gateway computer and of transmitting permission data based on the principal-authenticating credentials to the gateway computer; and
> one or more host computers operatively connected to the gateway computer and operating on any computer platform,
> wherein, based on the permission data, the gateway computer establishes a secure connection with at least one of the one or more host computers, and wherein the gateway computer transmits the one or more messages to at least one of the host computers over the secure connection.

Krajewski and Fisher, either taken alone or in combination, do not teach or suggest such a system. For example, neither Krajewski nor Fischer describe "a gateway computer operatively connected to the client computer, the gateway computer receiving principal-authenticating credentials and the one or more messages from the client computer," "a validation computer

operatively connected to the gateway computer and capable of receiving the principal-authenticating credentials from the gateway computer and of transmitting permission data based on the principal-authenticating credentials to the gateway computer," and "one or more host computers operatively connected to the gateway computer and operating on any computer platform," as recited in claim 24. As noted above in discussing Krajewski and Fischer, neither reference describe a "gateway computer" that is interposed between a client computer, a validation computer and one or more host computers, as recited in the claim.

Based on the foregoing, Applicant believes claim 24 to be patentable over Krajewski and/or Fischer, and respectfully requests that the Examiner withdraw the rejection of claim 24. As claims 25-28 depend from claim 24, and therefore include all of the limitations of claim 24, Applicant believes claims 25-28 to be patentable over Krajewski and/or Fischer for at least the same reasons as claim 24, and therefore respectfully requests that the Examiner withdraw the rejections of claims 25-28 as well.

In further contrast to Krajewski and Fischer, claim 29 recites a computer system that includes:

> a client computer for transmitting principal-authenticating credentials and a message;
>
> a gateway computer operatively connected to the client computer, the gateway computer receiving the principal-authenticating credentials and the message from the client computer;
>
> a validation computer operatively connected to the gateway computer and capable of receiving the principal-authenticating credentials from the gateway computer and of transmitting permission data based on the principal-authenticating credentials to the gateway computer; and
>
> one or more host computers operatively connected to the gateway computer and operating on any computer platform,
>
> wherein, based on the permission data, the gateway computer establishes a secure connection with the host computer, and transmits the message to the host computer over the secure connection.

Krajewski and Fisher, either taken alone or in combination, do not teach or suggest such a system. For example, neither Krajewski nor Fischer describe "a gateway computer operatively connected to the client computer, the gateway computer receiving the principal-authenticating credentials and the message from the client computer," "a validation computer operatively connected to the gateway computer and capable of receiving the principal-authenticating

credentials from the gateway computer and of transmitting permission data based on the principal-authenticating credentials to the gateway computer," and "one or more host computers operatively connected to the gateway computer and operating on any computer platform, wherein, based on the permission data, the gateway computer establishes a secure connection with the host computer, and transmits the message to the host computer over the secure connection" as recited in claim 29. As noted with respect to claim 24 above, Krajewski and Fischer do not describe a "gateway computer" that is interposed between a client computer, a validation computer and one or more host computers, as recited in the claim.

Based on the foregoing, Applicant believes claim 29 to be patentable over Krajewski and/or Fischer, and respectfully requests that the Examiner withdraw the rejection of claim 29. As claims 30-35 depend from claim 29, and therefore include all of the limitations of claim 29, Applicant believes claims 30-35 to be patentable over Krajewski and/or Fischer for at least the same reasons as claim 29, and therefore respectfully requests that the Examiner withdraw the rejections of claims 30-35 as well.

CONCLUSION

In view of the foregoing, Applicant respectfully submits that the pending claims are in condition for allowance. Reconsideration and allowance are respectfully requested. If there are any outstanding issues which need to be resolved to place the application in condition for allowance, the Examiner is invited to contact Applicant's undersigned representative by phone at the number indicated below to discuss such issues. To the extent necessary, a petition for extension of time under 37 C.F.R. § 1.136 is hereby made, the fee for which should be charged to deposit account number 07-2347. With respect to this application, please charge any other necessary fees and credit any overpayment to that account.

Respectfully submitted,

January 10, 2006

Joseph R. Palmieri
Reg. No. 40,760

Verizon Corporate Services Group Inc.
600 Hidden Ridge Drive
Mail Code: HQE03H14
Irving, Texas 75038
(972) 718-4800

Customer Number 32127